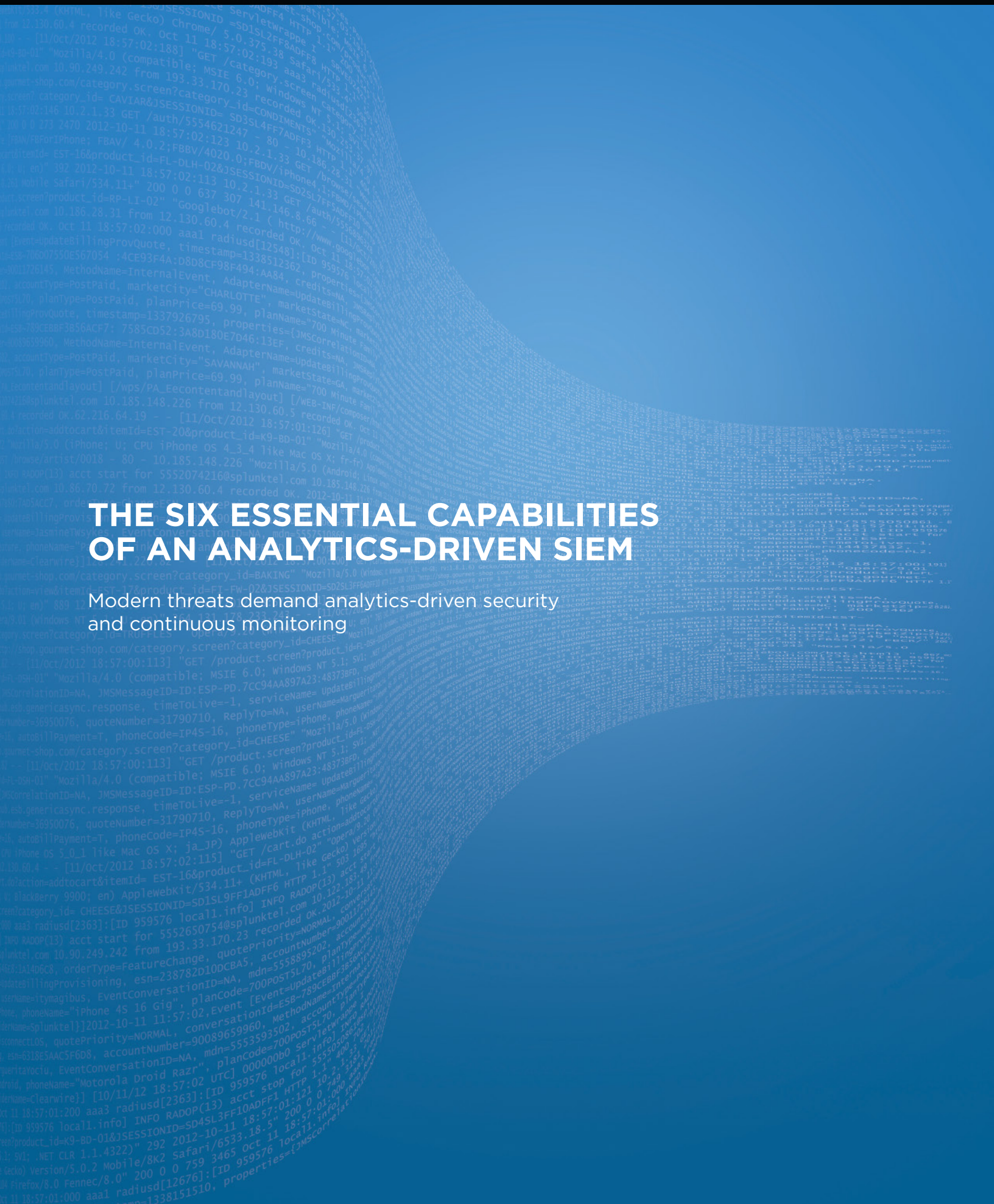
splunk>

WHITE PAPER

THE SIX ESSENTIAL CAPABILITIES OF AN ANALYTICS-DRIVEN SIEM

Modern threats demand analytics-driven security and continuous monitoring



Legacy SIEMs are Stuck in the Past

Finding a mechanism to collect, store and analyze security only data is relatively simple. There is no shortage of options for storing data. Collecting all security relevant data and turning all that data into actionable intelligence, however, is a whole other matter.

Many enterprise IT organizations that invested in security event information management (SIEM) platforms have discovered this fundamental truth the hard way. After spending a significant amount of time and money to record security events, the trouble is that not only did it take a long time to ingest all that data, but the underlying data system used to create the SIEM tends to be static.

Worse yet, the data available to analyze is based only on security events. That makes it difficult to correlate security events against what's occurring across the rest of an IT environment. When there's an issue, investigating a security event takes precious time most IT organizations can't afford. In addition, the SIEM system can't keep pace with the rate at which security events need to be investigated. The continued adoption of cloud services expands the threat vectors and enterprises now needed to monitor user activity, behavior, application access across key cloud and SaaS services, as well as on-premise services, to determine the full scope of potential threats and attacks.

What enterprise IT requires today is a simple way to correlate information across all security relevant data that enables them to manage their security posture. Instead of merely watching events after they occur, an IT organization should anticipate their occurrence and implement measures to limit their vulnerability in real time. For that, enterprises need an analytics-driven SIEM platform.

An analytics-driven SIEM allows IT to monitor threats in real time and respond quickly to incidents so that damage can be avoided or limited. But not all attacks are external—IT needs a way to monitor user activity so that it can minimize the risks from insider threat or accidental compromise. Threat intelligence is critical to understand the nature of the broader threat environment and put those threats into context for the organization. An analytics-driven SIEM must naturally excel at security analytics, giving IT teams the power to use sophisticated quantitative methods to gain insight into and prioritize efforts. Finally, a SIEM today must include the specialized tools needed to combat advanced threats as part of the core platform.

There are six essential capabilities of an analytics-driven SIEM:

Essential Capabilities of an Analytics-Driven SIEM	
Real-Time Monitoring	Threats can move quickly, and IT needs the ability to monitor threats and correlate events in real time to find and stop threats faster.
Incident Response	IT needs an organized way to address and manage potential breach as well as the aftermath of a security breach or attack in order to limit damage and reduce recovery time and cost.
User Monitoring	Monitoring user activity with context is critical to pinpoint breaches and uncover misuse. Privileged user monitoring is a common requirement for compliance reporting.
Threat Intelligence	Threat intelligence can help IT recognize abnormal activity, assess the risk to the business, and prioritize the response.
Advanced Analytics	Analytics are key to producing insights from mountains of data, and machine learning can automate this analysis to identify hidden threats.
Advanced Threat Detection	Security professionals need specialized tools to monitor, analyze and detect threats across the kill chain.

These capabilities give organizations the ability to use their SIEM for a wide range use of security use cases, as well as compliance. Let's take a deeper look at each key capability of an analytics-driven SIEM.

Real-Time Monitoring

The longer it takes to discover a threat, the more damage it can potentially inflict. IT organizations need a SIEM that includes monitoring capabilities that can be applied in real time to any data set, regardless of whether it's located on-premises or in the cloud. In addition, that monitoring capability needs to be able to retrieve both contextual data feeds such as asset data and identity data, as well as threat intelligence feeds, which can be used to produce alerts.

An analytics-driven SIEM needs to able to identify all the entities in the IT environment, including users, devices and applications as well as any activity not specifically attached to an identity. A SIEM should be able to use that data in real time to identify a broad range of different types and classes of anomalous behavior. Once identified, that data needs to then be easily fed into workflow that has been set up to assess the potential risk to the business that anomaly might represent.

There should be a library of predefined and customizable correlation rules, a security console to provide a real-time presentation of security incidents and events, and dashboards to provide real-time visualizations of ongoing threat activity.

Finally, all those capabilities should be augmented with out-of-the-box correlation searches that can be invoked in real time or schedule to regularly run at a specific time. Just as relevant, these searches should be available via an intuitive user interface that eliminates the need for IT administrators to master a search language.

Finally, an analytics-driven SIEM needs to provide the ability to search real-time and historical data locally in a way that serves to reduce the amount of network traffic accessing search data on-premise or Cloud or both.

Incident Response

At the core of any effective incident response strategy is a robust SIEM platform that makes it possible not only to identify distinct incidents, but also provide the means to track and reassign them as well as add annotations.

IT should be able to provide other members of the organization with varying levels of access based on their roles. Other key capabilities include the ability to either manually or automatically aggregates events, support for application programming interfaces (APIs) that can be used to pull data from or push information to third-party systems, an ability to gather legally admissible forensics evidence, and playbooks that provide organizations with guidance on how to respond to specific types of incidents.

Most importantly, an analytics-driven SIEM needs to include auto-response capabilities that can disrupt cyberattacks in progress.

In effect, the SIEM platform needs to be the hub around which a customizable workflow for managing incidents can be crafted. Of course, not every incident has the same level of urgency attached to it. An analytics-driven SIEM platform provides IT organizations with the means to categorize the severity of any potential threat. Via dashboards that can be used to triage new notable events, assign events to analysts for review, and examine notable event details for investigative leads, an analytics-driven SIEM arms IT organizations with the contextual insight needed to determine the appropriate response to any event.

Those response capabilities should include the ability to identify notable events and their status, indicate the severity of events, start a remediation process, and provide an audit of the entire process surrounding that incident.

Finally, the IT team should have a dashboard where they can intuitively apply filters to any field during an investigation to expand or reduce the scope of analysis with a few clicks of their mouse. The end goal should be nothing less than enabling any security team member to place events, actions and annotations into a timeline that makes it simple for other members of the team to easily comprehend what its occurring. Those timelines can then be

included in a journal that makes it simple to review attacks and to implement a repeatable kill chain methodology to deal with specific types events.

User Monitoring

At a bare minimum, user activity monitoring needs to include the ability to analyze access and authentication data, establish user context and provide alerts relating to suspicious behavior and violations of corporate and regulatory policies.

It's critically important that user monitoring be extended to privileged users who are most often the targets of attacks, and when compromised, wind up doing the most damage. In fact, because of this risk, privileged user monitoring is a common requirement for compliance reporting in most regulated industries.

Achieving those goals requires real-time views and reporting capabilities capable of leveraging a variety of identity mechanisms that can be extended to include any number of third-party applications and services.

Threat Intelligence

An analytics-driven SIEM must provide two distinct forms of threat intelligence. The first involves leveraging threat intelligence services that provide current information on indicators of compromise, adversary tactics, techniques and procedures, alongside additional context for various types of incidents and activities. This intelligence makes it easier to recognize abnormal activity such as, for example, identifying outbound connections to an external IP address known to be an active command-and-control server. With this level of threat intelligence, analysts have the information needed to assess the risks, impact and objectives of an attack that are critical to prioritizing an appropriate response.

The second form of intelligence involves assessing asset criticality, usage, connectivity, ownership, and, finally, the user's role, responsibility and employment status. That additional context is often critical when it comes to evaluating and analyzing the risk and potential impact of an incident. For example, an analytics-driven SIEM should be able to ingest employee badging information and then correlate that data with VPN authentication logs to provide context on an employee's location on the corporate network. To provide even deeper levels of analysis and Operational Intelligence, a SIEM also should be able leverage REST APIs to retrieve via workflow action or script to bring it into a system as well as combine structured data from relational databases with machine data.

Threat intelligence data ideally should be integrated with machine data generated by various types of IT infrastructure and applications to create watch lists, correlation rules and queries in ways that increase the success rate of early breach detection. That information should be automatically correlated with event data and added to dashboard views and reports or forwarded to devices such as firewalls or intrusion prevention systems that can then remediate the vulnerability in question.

The dashboard provided by the SIEM should be able track the status and activity of the vulnerability detection products deployed in the IT environment, including providing health checks of scanning systems and the ability to identify systems that are no longer being scanned for vulnerabilities.

In short, a comprehensive threat intelligence overlay needs to provide support for any threat list, automatically identify redundant intelligence, identify and prioritize threats that have been listed in multiple threat lists, and assign weights to various threats to identify the real risk they represent to the business.

Advanced Analytics

An analytics-driven SIEM provides advanced analytics by employing sophisticated quantitative methods, such as statistics, descriptive and predictive data mining, machine learning, simulation and optimization, to produce additional critical insights. Key advanced analytics methods include anomaly detection, peer group profiling and entity relationship modeling.

Just as significantly, an analytics-driven SIEM needs to provide tools that make it possible to visualize and correlate data by, for example, mapping categorized events against a kill chain or creating heat maps to better support incident investigations.

Making all that possible requires access to a SIEM platform that makes use of machine learning algorithms capable of learning on their own what represent normal behavior versus an actual anomaly.

That level of behavioral analytics can then be used to build, validate and deploy predictive models. It should even be feasible to employ model created using third-party tools in the SIEM platform.

Advanced Threat Detection

Security threats continually evolve. An analytics-driven SIEM can adapt to new advanced threats by implementing network security monitoring, endpoint detection and response sandboxing and behavior analytics in combination with one another to identify and quarantine new potential threats. Most firewalls and intrusion protection systems can't provide these capabilities on their own.

The goal should be not only to detect threats, but also to determine the scope of those threats by identifying where a specific advance threat may have moved to after being initially detected, how that threat should be contained, and how information should be shared.

In total, an analytics-driven SIEM should be able to correlate defenses across different styles of advanced persistent threat defenses.

A SIEM That Drives Actionable Intelligence

SIEMs offer a lot of promise, but legacy SIEMs simply can't keep up with the rate and sophistication of today's cyberattacks.

Organizations today require access to analytics-driven SIEMs that combine a big data platform optimized for machine data with advanced analytics, threat detection, monitoring tools, incident response tools and multiple forms of threat intelligence. Without those critical capabilities, IT is always going to be at a fundamental disadvantage when it comes to defending the IT environment from cybercriminals, who are working on behalf of organized crime syndicates and nation-states and have virtually unlimited resources at their disposal.

One of the best ways to combat those threats is to leverage an analytics-driven SIEM, which can combine IT operational data and security intelligence in a way that make it possible to identify the specific vulnerability these organizations are trying to exploit in real time. Armed with that data, IT security teams can remediate known threats better and proactively respond to new threats in real time to minimize any potential damage to the organization. It's a far cry from a legacy SIEM that collects security events without any means to turn that data into truly actionable intelligence.

The simple fact is that most IT organizations are evaluated on their ability to mitigate these attacks, but there's very little that can be done to prevent cybercriminals from launching these attacks. Worse yet, most IT organizations simply don't have the manpower to keep up with those attacks on their own. The difference between that attacks being a routine annoyance versus a catastrophic event invariably comes down to the robustness of an organization's SIEM platform.

The good news is that setting up an analytics-driven SIEM is easier than ever. Add to that the sophistication that a modern SIEM can now apply to defending the IT environment and it quickly becomes not a question of whether an IT organization needs a SIEM, but rather how quickly can it be implemented before the next wave of cyberattacks get launched.

Are you interested in learning the essential capabilities needed for an analytics-driven SIEM? **Learn about Gartner's critical capabilities for a SIEM and why it named Splunk a leader** for the fourth consecutive year.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com